RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

FACULTAD DE INGENIERIA
PROGRAMA DE ESPECIALIZACION DE SEGURIDAD EN REDES
ESPECIALIZACIÓN DE SEGURIDAD EN REDES
BOGOTÁ D.C.

AÑO DE ELABORACIÓN: 2015

TÍTULO: GUÍA PARA VALIDAR EL NIVEL DE SEGURIDAD DE LOS PERMISOS Y USO DE RECURSOS DE UNA APLICACIÓN MÓVIL BAJO PLATAFORMAS ANDROID

AUTOR (ES): HERNÁNDEZ VEGA, Marien, TORO SÁNCHEZ Crisitan Giovanny y VARGAS CARVAJAL Jesús Alfredo.

DIRECTOR(ES)/ASESOR(ES):

Carrillo Contreras Jorge Enrique, Velandia Jhon.

MODALIDAD:

PÁGINAS: 70 **TABLAS:** 3 **CUADROS:** 0 **FIGURAS:** 14 **ANEXOS:** 6

CONTENIDO:

PALABRAS CLAVES: Android, Aplicación móvil, Control, Evaluación, Infraestructura tecnológica, Permisos, Riesgo, Seguridad de la Información, Vulnerabilidad, Amenazas o ataques (Threats), Man in the middle

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

DESCRIPCIÓN: La presente guía, validar el nivel de seguridad de un App móvil y está diseñada con base en el aprendizaje adquirido en la especialización en Seguridad en redes de la Universidad Católica de Colombia.

El propósito de la guía es brindar una herramienta a las organizaciones, que permita establecer un nivel de confiabilidad aceptable para la validación, identificación, análisis y evaluación de los niveles de seguridad de una App Móvil cuando esta última se pretende lanzar en una organización como apoyo tecnológico a las actividades, y así establecer si esta puede ser enviada a producción o no; la guía está diseñada con base en estándares internacionales reconocidos y orientados a las App móviles, como son la norma ISO 27001 y NIST 800-163, que brindan la directriz necesaria para orientar la guía de manera clara y estandarizada, cumpliendo las pautas internacionales en seguridad y permitiendo que cualquier empresa, de cualquier tamaño e independientemente de su cur de negocio pueda hacer uso de esta, en un proceso de validación o implementación de la norma ISO 27001

METODOLOGÍA: El diseño metodológico de este trabajo se basa en la metodología PHVA (Planear, Hacer, Verificar y Actuar) de la norma ISO 27001 para los SGSI.

CONCLUSIONES: Al analizar la norma NIST 800-163 y caracterizar las vulnerabilidades que se pueden presentar en una aplicación móvil, las relacionadas con la integridad de la información son las más latentes a presentarse.

El desarrollo de App para organizaciones, debe ser validado de manera adecuada y cumpliendo cada uno de los procesos indicados por la Norma NIST 800-163 y por la guía indicada en este proyecto; pero una vez la App sea liberada y puesta en producción, se debe adicionalmente capacitar a los usuarios para que no incurran en cometer errores que puedan ocasionar fugas de información y las vulnerabilidades se puedan materializar.

La norma ISO 27001:2013, es un estándar a seguir en la implementación de la seguridad de la información, sin embargo a la hora de validar los controles relacionados a las aplicaciones móviles, no es tan específica y deja a interpretación del usuario final en buen proceder en este tipo de tecnologías.

Sin importar la cantidad de controles que la norma señale que deben existir, la actividad humana sobre los controles tiene gran influencia, ya que es una de las vulnerabilidades más atacadas.

Debe existir una relación costo beneficio al momento de implementar los controles que se crean necesarios para minimizar el riesgo de que las vulnerabilidades se materialicen, pues no es óptimo establecer controles que afecten de manera significativa la inversión de las organizaciones.

Se desarrolla una guía bajo el apoyo de la norma NIST 800-163, donde se encuentran vulnerabilidades orientadas a las App, pero se deben tener presentes los repositorios donde se encuentran otra serie de vulnerabilidades, para poder tener un proceso de validación de las App sólido.

La guía propuesta, fue de buena aceptación en la entidad aplicada, no solo porque es un procedimiento más organizado y metódico, sino porque crea conciencia en la administración de la seguridad de la información y a la misma entidad en procedimientos de calidad y validación periódicos sobre las tecnologías de información usadas en la organización.

Aplicar la guía desarrollada a una App permitió establecer la cantidad posible de vulnerabilidades en donde puede existir fuga de información o perdida de la misma, con el fin de identificar las recomendaciones sugeridas bajo la norma ISO 27001:2013.

FUENTES:

Agustín López Neira, J. R. (s.f.). *ISO27000.ES*. Obtenido de ISO27000.ES: http://www.iso27000.es

calidad, A. e. (2015). *Seguridad de la información*. Obtenido de QAEC: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

CVE - Common Vulnerabilities and Exposures. (2011). *Common Vulnerabilities and Exposures*. Obtenido de Common Vulnerabilities and Exposures: https://cve.mitre.org/

David Galisteo Cantero, R. M. (s.f.). *Man in the middle.* Obtenido de Seguridad en TIC: http://ns2.elhacker.net/MITM.pdf

Defición.MX. (12 de 10 de 2015). *Defición.MX.* Obtenido de Defición.MX: http://definicion.mx/proceso/

ESET. (2014). *Guía de seguridad para usuarios de Smartphones.*

EUMED. (2015). *Autenticación*. Obtenido de EUMED: http://www.eumed.net/cursecon/ecoinet/seguridad/autentificacion.htm

Eumed.net. (01 de 10 de 2015). *Eumed.net*. Obtenido de Eumed.net: http://www.eumed.net/cursecon/ecoinet/seguridad/autentificacion.htm

Galisteo Cantero, D., & Moya Reyes, R. (2009). *Man in the Middle - Ataque y Detección.*

Gelbstein, D. (2011). *Integridad de datos*. Obtenido de ISACA: http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

Gelbstein, D. E. (2011). La integridad de los datos: el aspecto más relegado de la seguridad de la información. *Isaca Journal, 6*, 6. Obtenido de ISACA: http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

INTECO. (20 de Marzo de 2012). *Estudio sobre seguridad en dispositivos móviles y Smartphones*. Obtenido de www.incibe.es: https://www.incibe.es/CERT/guias_estudios/Estudios//estudio_moviles_2C2011

Interactive Advertising Bureau - IAB. (30 de Septiembre de 2014). *IV Estudio Anual Mobile Marketing 2014.* Obtenido de http://www.iabspain.net/wp-content/uploads/downloads/2014/09/VI_Estudio_Anual_Mobile_Marketing_version_abierta1.pdf

IOACTIVE LABS. (8 de Enero de 2014). *Servicios de Seguridad IOACTIVE.* Obtenido de http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html

ITU. (agosto de 2009). *Aplicaciones móviles*. Obtenido de Unión Internacional de Telecomunicaciones: https://www.itu.int/net/itunews/issues/2009/06/04-es.aspx

Jaime, A. T. (2009). *Desarrollo de Aplicaciones para dispositivos móviles bajo la pplataforma Android de Google.* tesis, Universidad Carlos III de Madrird, Madrid.

Karpesky Lab Zao. (17 de Enero de 2014). *Karpesky Lab.* Obtenido de https://blog.kaspersky.es/vulnerabilidades-en-las-apps-bancarias-de-ios/2148/

Kaspersky. (2015). *Cifrado*. Obtenido de Kaspersky: http://latam.kaspersky.com/mx/internet-security-center/definitions/encryption

Maulini R., M. (Marzo de 2013). *Checklist de los procesos de autenticación e ingreso*. Obtenido de www.e-securing.com: http://www.e-securing.com/novedad.aspx?id=89

Mcafee. (Febrero de 2015). *http://www.mcafee.com.* Obtenido de http://www.mcafee.com/es/resources/reports/rp-quarterly-threat-q4-2014.pdf

MITRE. (s.f.). *Common Vulnerabilities and Exposures.* Obtenido de MITRE: http://makingsecuritymeasurable.mitre.org/docs/capec-intro-handout.pdf

National Vulnerability Database. (2014). *National Vulnerability Database*. Obtenido de National Vulnerability Database - NIST: https://nvd.nist.gov/

NIST. (01 de 10 de 2015). *National Institute of Standar and Tecnology*. Obtenido de http://scap.nist.gov/

NIST. (Febrero de 2015). *Vetting the Security of Mobile Applications (SP 800-163)*. Obtenido de http://dx.doi.org/10.6028/nist.sp.800-163

Rúben, C. M. (s.f.). *Tecnologías Moviles.*

Rubio, D. (2012). *Análisis De Seguridad De Aplicaciones Para Android.* España.

Salesforce . (2015). *Entornos Sandbox*. Obtenido de Salesforce : https://help.salesforce.com/apex/HTViewHelpDoc?id=data_sandbox_environments.htm&language=es

SCAP. (2015). *Security Content Automation Protocol* . Obtenido de SCAP: http://scap.nist.gov/

Wordpress. (2013). *https://protejete.wordpress.com*. Obtenido de Géstión de riesgos en la seguridad informátca: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

LISTA DE ANEXOS:

ANEXO 1: Guía para validar el nivel de seguridad de los permisos y uso de recursos de una aplicación móvil bajo plataformas Android.

ANEXO 1.A - CUESTIONARIO ISO 27001.

ANEXO A - CARACTERIZACIÓN DE VULNERABILIDADES.

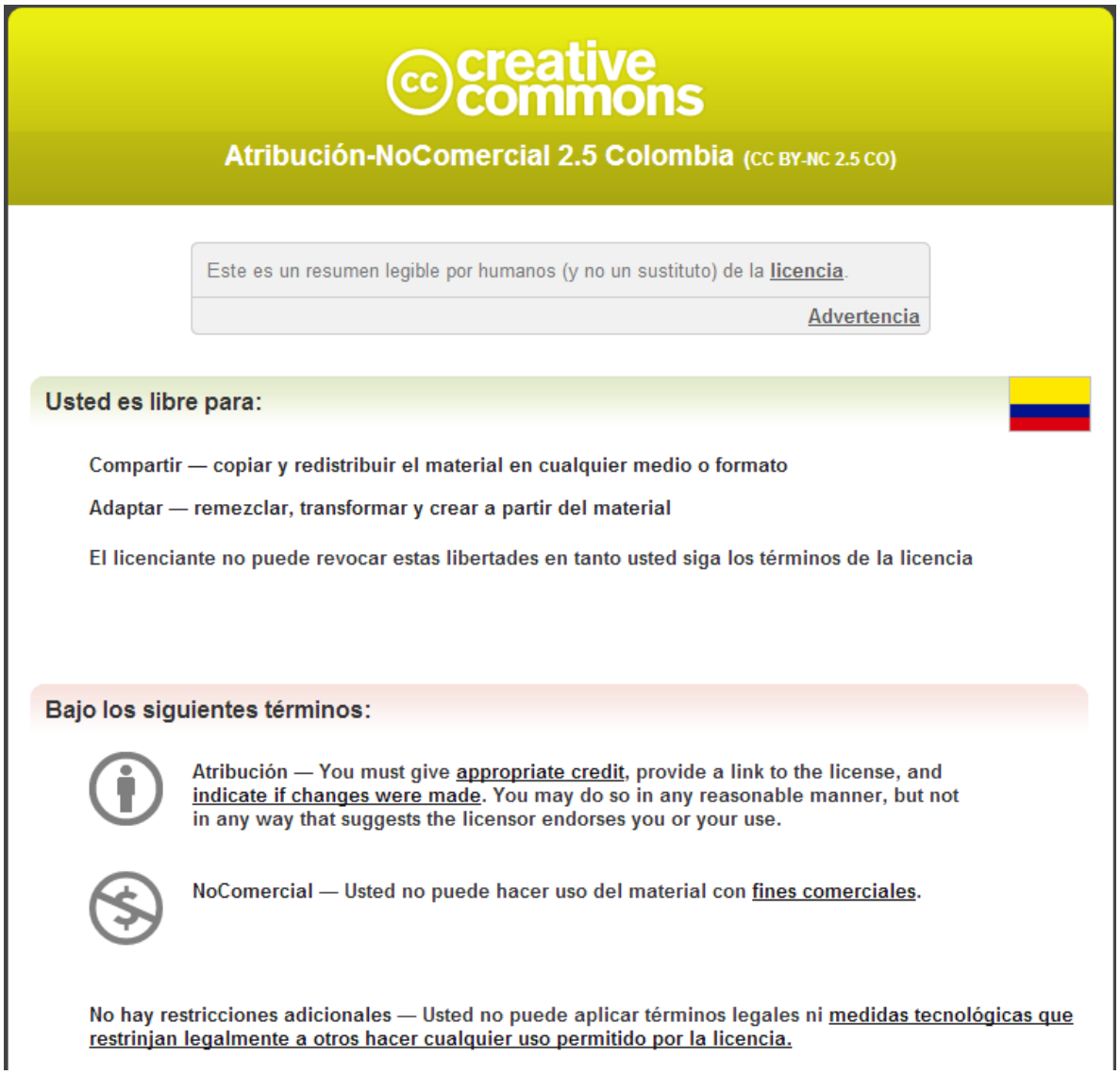
ANEXO B - CONTROLES DE SEGURIDAD APP.

ANEXO C - GUÍA DE SEGURIDAD PARA APP SOBRE ANDROID.

ANEXO D - CUESTIONARIO ISO 27001_APP_PQRSD.

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

TIPO DE LICENCIA



creative commons

Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5 CO)

Este es un resumen legible por humanos (y no un sustituto) de la licencia.

Advertencia

Usted es libre para:

Compartir — copiar y redistribuir el material en cualquier medio o formato

Adaptar — remezclar, transformar y crear a partir del material

El licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

Atribución — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NoComercial — Usted no puede hacer uso del material con fines comerciales.

No hay restricciones adicionales — Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.